

EDOK - Application for Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of:
Cell phones and other mobile devices in the
possession or control of DIXIE LEE
HARDIMAN

Case No. 21-MJ-356-DDB

APPLICATION FOR SEARCH WARRANT

I, Kevin B. Hall, Jr., a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the EASTERN District of OKLAHOMA (identify the person or describe property to be searched and give its location):

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

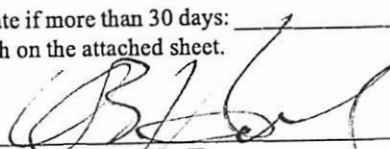
SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2, 3, 1001, and 2241, and the application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


KEVIN B. HALL, JR.
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: September 1, 2021

City and state: Muskogee, Oklahoma


JUDGE'S SIGNATURE
UNITED STATES MAGISTRATE JUDGE
Printed name and title



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kevin B. Hall, Jr., a Special Agent with Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), since September 2015, and am currently assigned to investigate Indian Country crime in the Durant Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at The FBI Academy in Quantico, Virginia and everyday work relating to conducting these types of investigations. I have received training in the area of investigating sexual abuse, and have had the opportunity to observe and review numerous cases involving sexual abuse as defined in 18 U.S.C. § 2241.

2. Prior to joining the Oklahoma City FO, I was assigned to the FBI - Chicago FO where I was designated as a Cyber Agent. As a Cyber Agent I received formal and on-the-job training in cyber-crime investigation techniques, computer evidence identification, and computer evidence seizure and processing. Through my training and experience, I have participated in the execution of search warrants for documents and other evidence, including computers and electronic media, in cases involving crimes the FBI is authorized to investigate. I am a federal law

enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2, 3, 1001, and 2241, and I am authorized by law to request a search warrant.

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for a mobile device specifically described in Attachment A of this Affidavit, including the content of the electronic storage device (the SUBJECT DEVICE) which is currently in the custody of the DIXIE LEE HARDIMAN for contraband, evidence, fruits, and instrumentalities, of violations of 18 U.S.C. §§ 2, 3, 1001, and 2241, which items are more specifically described in Attachment B of this Affidavit.

4. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2, 3, 1001, and 2241 are presently located in the SUBJECT DEVICE.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:
- a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

- b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).
- c. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- d. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters)

usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- e. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.
- f. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.
- g. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

- h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- i. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.
- j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- k. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.
- l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- m. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- n. A "sexual act," as defined in 18 U.S.C. § 2246(2), means (a) contact between the penis and vulva or the penis and the anus; (b) contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus; (c) penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person; or (d) the intentional touching, not through the clothing, of the genitalia of another person who has not attained the age of 16 years with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person.

- o. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.
- p. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.
- q. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

6. On or about 06/30/2021, I responded to the Idabel Police Department, 207 S. Central Avenue, Idabel, Oklahoma, 74745 and interviewed Dixie **HARDIMAN** (hereinafter referred to as **HARDIMAN**). At the time of the interview, **HARDIMAN** advised her phone number was 580-969-8536. **HARDIMAN** stated she witnessed the gang rape of her friend K.F. **HARDIMAN** advised in the late hours of 06/29/2021 into the early hours of 06/30/2021, K.F. and **HARDIMAN** were sitting at K.F.'s house when K.F. started to text people they knew to see if someone would be willing to pay them for sex without **HARDIMAN**'s knowledge. Around 12:00

AM on 06/30/2021 ZYLAN BAILEY (hereinafter referred to as BAILEY), Francisco Corona (hereinafter referred to CORONA, and RAY GOLSTON (hereinafter referred to GOLSTON) came to K.F.'s house. Eventually, according to **HARDIMAN**, K.F. and **HARDIMAN** agreed for K.F. to have sex with CORONA for \$300 and **HARDIMAN** to perform oral sex on GOLSTON and BAILEY for \$700, for a total of \$1,000. **HARDIMAN** made this statement after initially saying she did not know why CORONA, BAILEY, and GOLSTON came to K.F.'s house.

7. **HARDIMAN** advised K.F. and CORONA went into K.F.'s bedroom and **HARDIMAN** went into a separate room with GOLSTON and BAILEY. At some point, BAILEY and **HARDIMAN**, who had previously dated, started to talk. **HARDIMAN** said that, while they were talking, BAILEY pulled a gun on her, released the magazine, reinserted it, and pointed it at her head. **HARDIMAN** said that she believed it was possible he was joking and did not think he was actually going to shoot her. **HARDIMAN** stated that she then performed oral sex on BAILEY and GOLSTON, and after she was done, both BAILEY and GOLSTON went into K.F.'s bedroom and shut the door.

8. Within three minutes of BAILEY and GOLSTON going into the room with K.F. and CORONA, **HARDIMAN** heard K.F. making noises that sounded like K.F. was in pain. **HARDIMAN** stated she knew the difference between K.F.'s sounds of pleasure and pain because she and K.F. had been intimate in the past. After approximately 30 more seconds, **HARDIMAN** heard a crashing noise and CORONA, BAILEY, and GOSLTON ran out of K.F.'s bedroom. **HARDIMAN** said that while the men were running out of the room, K.F. yelled to **HARDIMAN** that CORONA, BAILEY, and GOLSTON had taken the \$1,000 that was previously left on a dresser for the sex, and only left \$4. **HARDIMAN** said the men were in K.F.'s room for

approximately 10 minutes in total. **HARDIMAN** advised that after the incident, K.F. made multiple statements about feeling dirty and feeling like she had been raped.

9. On or about 06/30/2021, K.F. was interviewed by Federal Bureau of Investigation Special Agent Kelly Foti. K.F. stated she did not agree to have sex with anyone and did not make any agreements to have sex for money. K.F. advised she was forced to have sex with **CORONA**, **GOLSTON**, and **BAILEY** after all three arrived at her house, uninvited, at approximately 10:00 PM on a Tuesday evening. When **CORONA**, **GOLSTON**, and **BAILEY** arrived at the home of K.F., K.F. recognized **CORONA** and **BAILEY**, although she did not have a close and continuing relationship with either man. K.F. advised me, she had never seen **GOLSTON** and did not know who he was when he arrived at her home. K.F. said **HARDIMAN** previously dated **BAILEY**, and **HARDIMAN** talked about **BAILEY** frequently. **HARDIMAN** confirmed a previous relationship with **BAILEY** in a deposition given in McCurtain County District Court by stating she and **BAILEY** “used to fuck.” K.F. and **HARDIMAN** were the only adults in the home. After being in K.F.’s home for approximately 10 – 20 minutes, **BAILEY** and **CORONA** forced K.F. to stay in her bedroom with them, and both men pointed pistols at her.

10. Additionally, while K.F. was borrowing **HARDIMAN**’s phone the day after she was raped, K.F. noticed that **HARDIMAN** had sent “Relk,” who was later identified as **JAYDEN RICHARDS**, a message that alluded to previous threats from **RICHARDS** about shooting at K.F.’s house. K.F. also saw in messages on **HARDIMAN**’s phone that **RICHARDS** alluded to **HARDIMAN** working with law enforcement by calling **HARDIMAN** a rat who was trying to set him up.

11. On or about 07/08/2021, **HARDIMAN** was deposed under oath in a Protective Order Hearing in McCurtain County District Court. I reviewed a transcript of **HARDIMAN**'s testimony and observed that she reiterated her claim that K.F. had sex with **GOLSTON**, **CORONA**, and **BAILEY** with the expectation that K.F. would receive money. **HARDIMAN** stated she knew that is why K.F. invited **GOLSTON**, **CORONA**, and **BAILEY** to the house. **HARDIMAN** stated in the deposition, contrary to the statements she provided to me, that she did not know the agreed-upon amount of money that was going to be exchanged for sex.

12. In the deposition, **HARDIMAN** advised that prior to the rape, K.F. invited **GOLSTON**, **CORONA**, and **BAILEY** into her bedroom at the same time and that during that time, and **HARDIMAN** did not believe K.F. was being raped. During the deposition, an attorney asked **HARDIMAN** whether it was true that either she or K.F. demanded that **CORONA**, **GOLSTON**, and **BAILEY** pay the original \$1,000 and an additional \$2,000 to keep K.F. from telling the police that the three men raped K.F. **HARDIMAN** agreed with the statement. **HARDIMAN** testified under oath that **GOLSTON**, **CORONA**, and **BAILEY** did not possess weapons, again contrary to her statements to me, and did not use any force.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

13. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers, mobile devices and digital technology are a primary way in which individuals interested in sexual assault interact with each other.
- b. Smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone

to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos and contain screenshots or recordings of messaging conversations.

c. Mobile devices such as smartphones may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world.

d. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. For example, multiple apps, allow users to privately message with each other.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE

was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.
- e. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- f. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

16. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

17. This warrant permits law enforcement to compel all individuals present at the SUBJECT PREMISES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive

camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked

using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

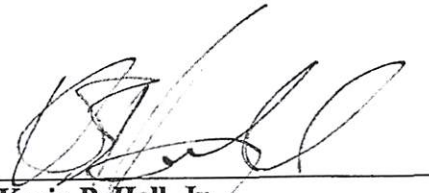
h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of **DIXIE LEE HARDIMAN** to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of **DIXIE LEE HARDIMAN** and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of **DIXIE LEE HARDIMAN** and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that **DIXIE LEE HARDIMAN** state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to ask **DIXIE LEE**

HARDIMAN to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

18. *Manner of execution.* Because the warrant for the SUBJECT DEVICE seeks only permission to seize and examine a device in the possession of DIXIE LEE HARDIMAN, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant for the SUBJECT DEVICE at any time in the day or night.

CONCLUSION

19. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the device described in Attachment A, authorizing the seizure and search of the items described in Attachment B.



Kevin B. Hall, Jr.
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 1st day of September, 2021.



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF DEVICE TO BE SEARCHED

All mobile devices in the possession and control of DIXIE LEE HARDIMAN, a self-identified white female who is 5'8" in height and weighs approximately 255 pounds and has a date of birth of 09/06/2002. DIXIE LEE HARDIMAN has a reported address of 303 E. Lucas Street in Valliant, Oklahoma, 74764 and phone number of 580-969-8536.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 2, 3, 1001, and/or 2241 and involve DIXIE LEE HARDIMAN, including:
 - a. Records of communications and interactions with K.F., CORONA, GOLSTON or BAILEY;
 - b. Evidence regarding when any pictures or videos sent to K.F., CORONA, GOLSTON, or BAILEY were taken;
 - c. Records of communications with others regarding K.F.;
 - d. Any evidence relating to DIXIE LEE HARDIMAN's schedule or travel.
2. For the cell phone whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "DEVICE"):
 - a. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
 - e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

- f. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;
- h. evidence of the times the DEVICE was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. records of or information about Internet Protocol addresses used by the DEVICE;
- k. records of or information about the location of DIXIE LEE HARDIMAN and the DEVICE;
- l. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

3. Records, information and items relating to violation of statutes described above including:

- a. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- b. Records and information showing access to and/or use of the device; and
- c. Records and information relating or pertaining to the identity of the person or persons using or associated with DIXIE LEE HARDIMAN.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic evidence.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.